2019 International Conference on Localization and GNSS (ICL-GNSS), 4-6 June 2019, Nuremberg, Germany
DOI: 10.1109/ICL-GNSS.2019.8752862

Vulnerability analysis of GPS receiver software

G. Mori Gonzalez
Altran Technologies
Toulouse, France

I. Petrunin
Cranfield University
Cranfield, United Kingdom

R. Zbikowski
Spirent
Crawley, United Kingdom

K. Voutsis
Spirent
Crawley, United Kingdom

R. Verdeguer Moreno
Spirent
Crawley, United Kingdom

***Abstract*—Satellite navigation systems such as the Global Positioning System (GPS) makes it possible for users to find their relative or absolute position. Thanks to its mobility and reliability, the GPS is used in many civil and military applications. However, the GPS does not provide an advanced level of security. Therefore, it could be potentially a target of attacks. With the development of new GPS attacks, the security knowledge has to grow at the same rate, so existing attacks can be detected by updated versions of receiver software or hardware. In this paper, a comparative analysis of GPS receiver resilience to software attacks is performed with the help of GNSS simulator from Spirent. The main objective of this work is to perform a sensitivity analysis of variables involved in calculation of position of the GPS receivers from different price bands that might be targeted by existing or future GPS attack. Variables making the biggest impact on calculated position are determined using the model. Experimentation validation of their influence is performed using selected receivers and corrupted signals generated by GNSS simulator. The testing is based on tuning the selected variables in order to simulate the theoretical error obtained from the sensitivity analysis. The results obtained from testing are discussed in order to analyse the behaviour of the considered GNSS receivers (including the premium class ones) and establish whether they provide a protection from existing or potential GPS attacks.**

***Index Terms*—GPS, Security, GNSS, RF Attacks, Spoofing, GSS 7000, Spirent**

I. Introduction

In a highly connected digital world, a reliable source for absolute positioning, navigation and timing (PNT) data is a clear need for many military and commercial applications. Global Navigation Satellite Systems (GNSS) are considered as an effective and efficient solution for most of these needs. According to the 2017 GNSS Market Report published by the European GNSS Agency [1], there are 5 billion GNSS devices in use around the world and 8 billion are forecast by 2020. There are multiple GNSS such as GLONASS [2], BeiDou [3] or Galileo [4]. Nevertheless, the most commonly used one is the Global Positioning System (GPS) [5].

This worldwide dependency on GNSS technology and its application to safety critical operations illustrates the need of an integrated and robust system. Notwithstanding, every system has its own vulnerabilities and ways to exploit them. In the past, GNSS have experienced both intentional and unintentional attacks mainly exemplified in jamming [6] and spoofing events [7, 8]. On the other hand, there are more sophisticated attacks than jamming and spoofing that can affect GNSS receivers. As seen in [9], many vulnerabilities can be found in a GPS receiver software. Attacks such as Middle-of-the-Earth, date desynchronization or specific operating system bugs are described in this paper and their consequences can be devastating depending on the receiver model.

All these attacks have triggered an extensive academic research together with software and firmware updates for commercial devices to meet the requirements of accuracy, integrity, continuity and availability in relevant applications. Significant resources are being spent every year to increase the security of these systems as described in works [10, 11, 12]. The most common attacks, such as jamming or spoofing pseudoranges, are already addressed by high quality receivers [13] using, for example, GNSS authentication which cannot be replicated as easily as the current public GPS signal. Hence, these attack vectors are not in the scope of this study.

In view of the present high interest to the improvement of the resilience of the GNSS receivers to different type of attacks, both present and future, the aim of this work is to investigate the sensitivity of the software part of a GPS receiver to the variation in the input variables that can be affected by various external reasons, including attacks on the GPS receiver. Novel results obtained here with use of the Spirent GSS7000 GNSS simulator and a number of commercially available receivers, allowing evaluation of their resilience to existing and potential attacks and discussing also challenges of such analysis.

II. Model and simulation

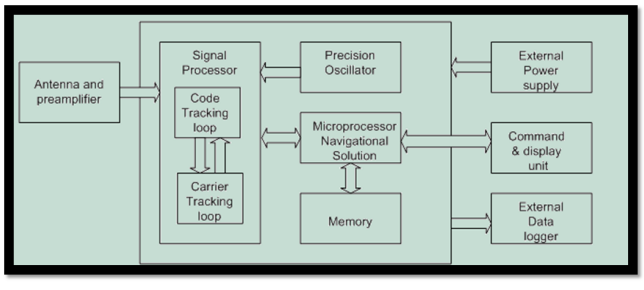

Fig. 1: Generic GPS receiver structure

The typical structure of the GPS receiver under test is shown in Fig.1. While attacks in general can target different blocks of the receiver to affect the position calculation,

effectiveness of these attacks depends on the hardware realisation of the block in that particular receiver. The main focus of this study is a more generic consideration of GPS calculations in the Microprocessor Navigational Solution block.

GPS PNT solutions rely on the ephemeris data of each satellite involved in the computations. That data is contained in the navigation message broadcast by satellites. Independent analysis of every parameter contained in the satellite's navigation message is not practical. Therefore, in order to achieve meaningful results using a time-affordable method, a sensitivity analysis of the GPS receiver inputs should be performed to assess the impact of each independent variable on the position output.

A. Navigational Solution Block Model

A model of the Navigational Solution Block is required to perform a sensitivity analysis. Therefore, a representative model has to be chosen to achieve realistic results. Even though an actual GPS receiver software would be the best option to perform the analysis, details of GPS receiver software structure are usually not available due to sensitivity of this information. This limitation led to the choice of an open-source software model. The chosen model is GoGPS, a software package designed to improve the positioning accuracy of GPS devices [14, 15]. The GoGPS model was originally developed in MatLab [16]. It takes the information contained in the digitized GPS RF signal as inputs and returns the messages in the format of National Marine Electronics Association (NMEA) that are produced by many commercial receivers. Subsequently, the model has been adapted to MatLab Simulink [17] making easier the access to all the variables present in the computations. The Simulink model is divided in four major blocks corresponding to the natural steps for obtaining a positioning solution from GPS signals described below:

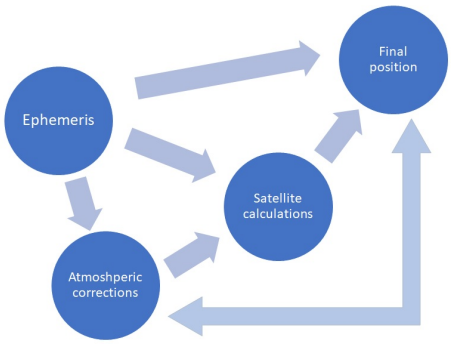

Fig. 2: GoGPS model diagram [14]

Input block of the model takes all the ephemeris and timing data that the receiver needs in order to calculate its position. More information about these variables can be found at Global Positioning System standard [5].

Atmospheric corrections block is subdivided into tropospheric and ionospheric corrections parts. Klobuchar model is used for the ionosphere modelling, reducing its induced error by 50% [18]. Saastamoinen algorithm [19] was used to recreate the tropospheric error. Improvements could be added to get better accuracy from these errors. However, a detailed study of the atmospheric corrections influence on the positioning accuracy is out of scope of this study.

Satellite calculations block represents the satellite position calculations. Firstly, the relativistic error due to the gravitational potential and the relative speed is calculated. This error has relatively low order of magnitude. However, it has a noticeable effect on the observed transmission time due to the signal propagation speed. Secondly, the Earth's rotation also has to be taken into consideration as during the transmission not only the satellite moves but the Earth does as well.

Position calculation block takes every calculated information from previous blocks in order to get the final position of the receiver.

B. Simulation procedure

It can be seen from the above description of the software blocks, some assumptions have been made. First, the ephemeris data values used as input are decimal values. Binary conversion is not made in the model, hence all the possible errors related to this transformation are not taken into account. Second, signal group delay is calculated from assumption of working with L1 signal of GPS constellation.

The output variable of the sensitivity analysis is the distance from the centre of the Earth to the GPS receiver. During the analysis the ephemeris input variables are changed one by one and variation in the output variable is logged. Only one satellite signal will be corrupted at a time. A possible simultaneous variation of multiple variables or multiple satellite signals corruption was not considered in this study.

The input variables are varying within specific ranges that depend on the variable itself and defined following GPS standard of Positioning Service Signal Specification [5]. The sensitivity analysis results are used then to perform an experimental validation as it will be described in the next section.

III. Results

The results of the sensitivity analysis using the GoGPS model [14] are obtained by Spirent software SimGen [20]. This software is able to control the simulated GNSS RF signals generated by the simulator for the most complicated GPS-based scenarios with inclusion of the satellite constellation related effects, e.g. satellite movement.

Spirent's SimGen software offers an opportunity to perform Receiver Autonomous Integrity Monitoring (RAIM) that ensures the GPS signal integrity by monitoring and analysing GPS measurements using redundant GPS signals [21].

Fig. 3: Experimental procedure

Since four satellites are needed to calculate the receiver position, for RAIM implementation at least five are needed to perform the comparison and detect a corrupted signal. This technology may not be always available as five or more healthy satellites must be available. In addition, RAIM is not included in the simulated model. Therefore, in order to make the experiments as similar as possible to the simulation, RAIM was disabled in GPS receivers for all experiments. An overview of the experimental procedure is outlined in Fig. 3.

Once the key variables are identified from the sensitivity analysis, experimental validation is the next step. This procedure allowing confirmation of the theoretical results from previous section using commercially available receivers. In order to recreate the scenario close to the one used in the sensitivity analysis, Spirent simulator GSS7000 [20] was used. This simulator allows creation of an RF signal, representing designed scenario of a corrupted signal which is fed to selected GPS receivers.

A. Sensitivity analysis results

The sensitivity analysis results show that three variables demonstrate the highest level of influence on the position calculation error: ω_0, $\dot{\omega}$ and $\sqrt{A}$. Other variables are not taken into account due to their low impact on the final position calculations, with ionospheric and tropospheric corrections making the smallest impact according to the model. The results are summarized in Table I:

TABLE I: Sensitivity analysis results

Variable	Description	Maximum error magnitude(m)	Error description	Range of values
$\sqrt{A}$	Square root of the semi major axis	10^{11}	Least square solution divided by zero	[2537, 6557]
ω_0	Longitude of ascending node of orbit plane at weekly epoch	10^{10}	Least square solution divided by zero	[-1,1]
$\dot{\omega}$	Rate of right ascension	10^{8}	Argument of latitude error augmentation	[-9,54e-07, 9,54e-07]

Figures 4, 5 and 6 show how the output variable (distance from the center of the Earth to the GPS receiver) varies with each input variable change. On the X axis, the value of each variable is shown as a percentage of their allowed range value. On the Y axis, the distance from the center of the Earth is shown in meters.

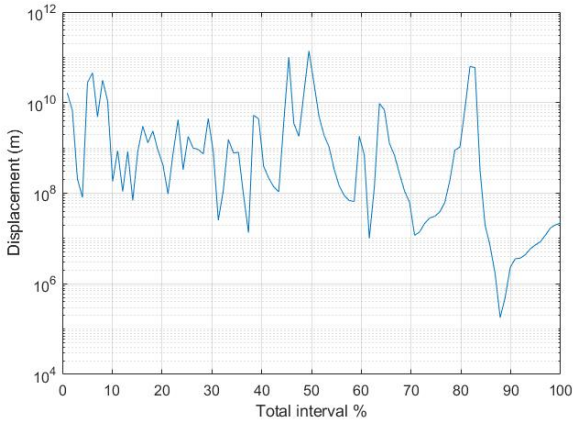

Fig. 4: Sensitivity Analysis Result: $\sqrt{A}$

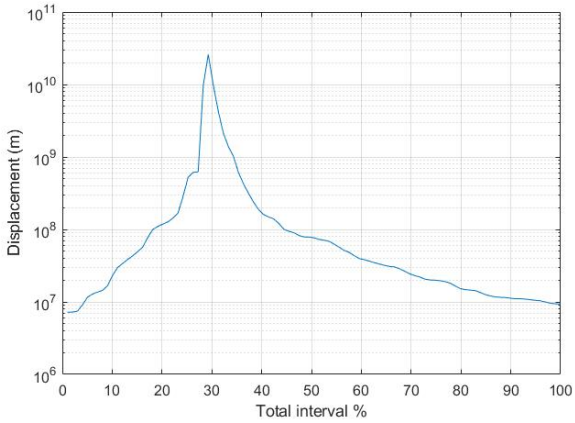

Fig. 5: Sensitivity Analysis Result: ω_0

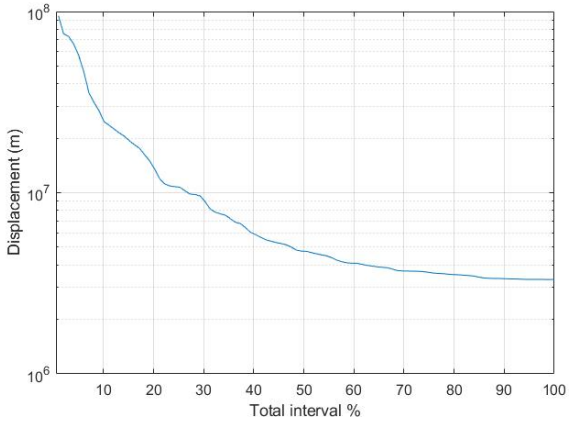

Fig. 6: Sensitivity Analysis Result: $\dot{\omega}$

Figures 4 and 5 show the effect of a corrupted value on the GPS least square solution position calculation. Corrupted values of $\sqrt{A}$ and ω_0 lead to problems in the least square solution calculation. The noise-like behaviour of the position error due to corrupted $\sqrt{A}$ Several peaks are found in the figure as the variable is used for only 1

satellite position calculation, which as an indirect effect on the final receiver position determination, including terms such as the relativistic clock error correction or the satellite orbit calculation. During these calculations, a division by zero makes the final position go to a very large number, creating large peak visible in Fig. 5.

Variable $\dot{\omega}$ is the 3rd in the list of selected variables with respect to the influence on position error. The error in $\dot{\omega}$ affects the latitude calculation. The error propagates through the receiver position calculation matrix and is amplified by the Earth radius. Therefore, increase in the value of this variable will lead to the variation shown in Fig 6. Details on the receiver position calculation matrix and corresponding calculations can be found in [5].

Other input variables that are not shown here have a lower impact on the solution; therefore, they have not been investigated further.

B. Experimental validation results

During the experiments four GPS receivers, both cheap and expensive models, were considered. The characteristics are summarised in the Table II, where horizontal accuracy is mentioned with and without using Satellite-based Augmentation System (SBAS) that improves the accuracy of position estimation and will have a big impact when performing small variable changes.

TABLE II: GPS Receiver details

Receiver (Rx)	Price (Eur)	H.Acc. (m)	SBAS H.Acc. (m)
Rx 1	12000	1.2	0.6
Rx 2	7000	2	0.5
Rx 3	70	2.5	N/A
Rx 4	30	2.5	2

For the experimental validation three input variables identified from the sensitivity analysis were uniformly sampled between their minimum and maximum values given by GPS signal specification [5]. In order to avoid over-the-air interference direct wired connection between the simulator and the GPS receiver was used.

Results of the validation were expressed in terms of the errors relative to true position: geodetic latitude, longitude and altitude (LLA) coordinates. For simplicity true position was set to (0,0) at the Earth surface. The errors were obtained by recording the maximum change of the position after the change in the input variable.

Once the variables were set, Spirent's PosApp application was used to create the scenario with the requested specifications.

IV. Analysis and Discussion

The position results are analyzed with respect to errors relative to the true position. An error is detected when the position error surpasses the tolerance defined by each receiver's accuracy specifications. Several types of errors can be defined based on the observed results. They differ by the possibility of the correction, correction source, time required for correction and behaviour of the error in time:

1) Errors that are detected and fixed by the receiver internally are denoted as "Error detected".
2) Errors that are fixed after some time e.g. after obtaining the almanac or in post-processing this error is denoted as "Temporary error".
3) Errors that increase in time are reflected in the tables as "Increasing Error".
4) Error combination is possible, as "Temporary increasing error" means an increasing error that is fixed in time.
5) If the position switches between the correct and the corrupted position for a certain amount of time to finally converge to the correct position, "Temporary alternating error" is used in the table.
6) If the error cannot be corrected with the full almanac data it is denoted in the Tables as "Permanent error".

The special case of the error is when receiver provides no solution. This indicates that the error was detected, but no solution is given to emphasize that the solution, even if it can be calculated, is not trustworthy. Tables III, IV and V summarizes the error performance of the analysed GPS receivers against modifications in three input variables identified from the sensitivity analysis using predefined types of errors: types 1 to type 6, according to the definition above) and also "No solution" category.

TABLE III: $\sqrt{A}$ effect

$\sqrt{A}$	8191	0	6000	5400
Rx 1	Error detected	Error detected	Error detected	No solution given
Rx 2	Error detected	Error detected	Temporary error	Temporary error
Rx 3	Error detected	Error detected	Error detected	Temporary alternating error
Rx 4	Error detected	Error detected	Temporary error	Temporary error

The colors of cells define the impact on the receiver calculated position: white means no impact (error corrected internally), yellow means a temporary impact and orange a permanent impact. The selected values are the maximum and minimum of each variable and values close to the one that gives the non-corrupted position. This way, extremes will be tested as well as little modifications.

TABLE IV: ω_0 effect

ω_0	-1	1	0	-0.018
Rx 1	Error detected	Error detected	Error detected	No solution given
Rx 2	Temporary error	Error detected	Error detected	No solution given
Rx 3	Temporary error	Error detected	Permanent error	Permanent error
Rx 4	Increasing error	Temporary increasing error	Temporary increasing error	Increasing error

TABLE V: $\dot{\omega}$ effect

$\dot{\omega}$	0	4.76e-7	3.72e-9	-9.5e-7
Rx 1	Error detected	Temporary increasing error	Increasing error	No solution given
Rx 2	Error detected	Temporary increasing error	Increasing error	Increasing error
Rx 3	Error detected	Temporary increasing error	Error detected	Increasing error
Rx 4	Increasing error	Temporary increasing error	Temporary increasing error	Increasing error

A. Analysis of parameter influence

Square root of A and ω_0 values are continuously monitored by the receivers. As they are key factors in the satellite orbits, an error in these variables can lead to a significant error in calculated position. This happens due to assuming that the satellite is in a different position from the true one; therefore, the transmission time will differ. This error will propagate through the receiver position calculations. The receiver is able to detect such misleading information by two different ways:

1) Analyze the range of variables. If the value of the input variable is out of the boundaries, the receiver can fix the input.
2) Detect and exclude of satellite ephemeris corrupted parameters by comparing them (integrity-checking) against the almanac data.

Position error due to corruption in $\dot{\omega}$ differs to the previous cases as it is a derivative variable. Hence, the input variable is multiplied by time and sensitivity of the output variable is not as straightforward as in previous cases. On the other hand, if the input variable value is out of range or differs from the almanac value by a big margin, the error will be detected the same way as it was done in the previous cases.

B. Comparison with simulation

When analyzing the experimental results, the comparison between the experimental and theoretical results is performed. Experimental results were calculated by obtaining the maximum difference in position by tuning each variable. Once the variables values that give the maximum error are selected, they are included in the simulated model and the error in position is calculated. These differences found are shown in the Table VI that shows the maximum error induced in the receivers by tuning each variable.

TABLE VI: Error comparison

Error, (m)	$\sqrt{A}$	ω_0	$\dot{\omega}$
Simulation	6000	80000	1500
Rx 1	N.S.	N.S.	188 + 0.2pmin*
Rx 2	2	15*	60 + 0.3 pmin*
Rx 3	2	160	0.4 pmin
Rx 4	0.15	0.5	510

In this table, "pmin" means per minute and * means that the error may be fixed in time depending on the satellite constellation changes. The corrupted satellite may go out of range from the receiver. This would fix its position calculation automatically because other, good satellite data is used.

In general differences between errors in receivers outputs and simulation results can be explained in first place by absence of exact information about the GPS receiver firmware that is a commercially sensitive information and it is not disclosed by manufacturers. Other reasons can be also given:

- Differences between simulation and experimentation scenarios, e.g. the time variability or the number of satellites. The final error in commercial receivers will vary depending on the number of available satellites. This is not realised in the Simulink model.
- Implemented GPS model is not able to process almanac data from other satellites during the simulation. This information is used by real receivers to check the received information from direct satellite communications. In addition, the receivers are able to perform a variable comparison between satellites, detecting rapid changes due to GPS attacks or instabilities and banning the problematic satellites.
- Numerical errors can be fixed in commercial GPS receivers. This characteristic is not present in the GPS model for simulation.

Post-processing is extensively used in commercially available GPS receivers. Position errors based on computational issues such as the ones found in $\sqrt{A}$ and ω_0 are not affecting experimentally investigated receivers, which have methods to avoid these kind of errors. In addition, $\sqrt{A}$ is a variable whose corruption was already known in the past as "Middle-Earth Attack".

GPS receivers are checking the variables against the expected values. An initial comparison with the variable limiting range is performed, followed by the almanac data comparison. If any of these checks result in detecting of a corrupted variable, the general behaviour is to exclude the corrupted satellite from the position calculation.

Error based on derivative error propagation essentially affects the experimental receivers. The order of magnitude between the experimental and theoretical error does not differ as much as in previous cases. In addition, this case has an extra difference between theoretical and experimental: the GPS model error is fixed in time, while the error from the experimental model raises with time. Therefore, if the experiment was given infinite time and post-processing is not used, the error would match the theoretical one.

As an example, the corruption of $\dot{\omega}$ is maximized when it is equal to zero, as shown in Fig. 6. This fact affects all receivers and, in case of receiver 4, the position error exceeds 500 m (see table VI). The error in the receiver output is within an order of magnitude difference from the simulation results, that can be considered as relatively good match, providing that model did not have any internal error corrections.

GPS receivers' dependency on almanac data can be exploited as well. Potentially, the overall constellation can be blocked and a new one can be simulated and broadcasted. Therefore, almanac checking can be overcome.

V. Conclusions

By the comparison with the simulated results it was found that many receivers are able to handle signals with corrupted information on semi major axis ($\sqrt{A}$), minimizing the position error or providing an indication of the corruption by means of refusing to give a solution. It can be seen from the results that this is due to extensive internal post-processing of the results that allows to detect and in many cases to correct an error.

The other two parameters: ω_0 and $\dot{\omega}$ present significant challenge to receivers in case of their corruption. The error in position in these cases may reach hundreds of meters and in case of $\dot{\omega}$ corruption may also increase with time. Even when solution can be obtained it is frequently takes longer to produce it.

It is not surprising that abilities of the receivers to handle corruption of variables are depending on their price. Cheaper Receivers 3 and 4 have more faulty cases in comparison to more expensive Receivers 1 and 2. Receiver 2 is the one that is able to fix many errors. However, it is not able to detect certain types of corruption. Hence, this receiver is ideal for non-critical applications where an error is not catastrophic. Receiver 1 has a really good capacity to detect errors. The results show that it is able to detect errors even if it is not able to fix them. The method of detection is unknown though due to the lack of knowledge about the receiver's firmware. This receiver is ideal for critical applications as it is able to cope with the majority of the input corruption.

This work can be continued in the future by improving the model used for sensitivity analysis in terms of its accuracy, handling almanac data and use of multiple satellites for error reduction. The updated model can become a useful tool for detecting existing vulnerabilities through enhanced sensitivity analysis and developing solutions for error detection and correction for future GNSS receivers.

References

[1] "GNSS market report issue 5," European Global Navigation Satellite Systems Agency, Tech. Rep., 2017.

[2] "Global navigation satellite system GLONASS (in Russian)," Russian Federation, Moscow, Tech. Rep., 2008.

[3] "Beidou navigation satellite system signal in space," China Satellite Navigation Office, Tech. Rep., 2013.

[4] "Galileo satellite navigation system," European Parlament, Tech. Rep., 2018.

[5] *Global positioning system standard Positioning Service Signal Specification*, 2nd ed. GPS NAVSTAR, USA, 1995.

[6] J. Coffed, "The threat of GPS jamming," *Clifton, NJ, Exelis*, 2014.

[7] J. Nielsen, G. Lachapelle, A. Jafarnia, and A. Broumandan, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Techniques, International Journal of Navigation and Observation*, vol. 1, Article ID 127072, pp. 1–16, 2012.

[8] D. Shepard, A. Kerns, T. Humphreys, and J. Bhatti, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 34, no. 4, pp. 617–636, 2014.

[9] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," *Proceedings of the 2012 ACM conference on Computer and communications security*, October 2012.

[10] J. Warner and R. Johnston, "GPS spoofing countermeasures," *Homeland Security Journal*, 2003.

[11] Engineering Royal Academy, "Global navigation space systems: Reliance and vulnerabilities," 2011.

[12] A. Purwar, D. Joshi, and V. K. Chaubey, "GPS signal jamming and anti-jamming strategy - a theoretical analysis," *IEEE Annual India Conference (INDICON)*, pp. 1–6, 2016.

[13] K. Liu, W. Wu, Z. Wu, L. He, and K. Tang, "Spoofing detection algorithm based on pseudorange differences," *Sensors*, vol. 18, no. 10, 2018.

[14] E. Realini, M. Reguzzoni, A. Dominioni, and M. Colla, "GoGPS model," http://www.gogps-project.org/, 2016.

[15] R. Teruzzi, E. Realini, M. Reguzzoni, A. Dominioni, and M. Colla, "GoGPS documentation," *University of Milano*, 2016.

[16] MathWorks, "Matlab documentation," *https://uk.mathworks.com/help/matlab/*, 2018.

[17] MathWorks, "Simulink documentation," *https://uk.mathworks.com/help/simulink/*, 2018.

[18] N. Wang, Y. Yuan, Z. Li, and X. Huo, "Improvement of klobuchar model for GNSS single-frequency ionospheric delay corrections," *Advances in Space Research*, vol. 57, no. 7, pp. 1555–1569, April 2016.

[19] J. Saastamoinen, "Contributions to the theory of atmospheric refraction, part II. refraction corrections in satellite geodesy," *Bulletin Geodesique*, vol. 107, no. 1, pp. 13–34, 1973.

[20] *SimGen software user manual*. Spirent, 2016.

[21] J. Blanch, T. Walter, Y. Lee, B. Pervan, M. Rippl, and A. Spletter, "Advanced RAIM user algorithm description: Integrity support message processing, fault detection, exclusion, and protection level calculation," in *25th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS)*. Standford University, 2012, pp. 2828–2849.

2019-07-04

Vulnerability analysis of GPS receiver software

Gonzalez, G. Mori

IEEE

Mori GG, Petrunin I, Zbikowski R, et al., (2019) Vulnerability analysis of GPS receiver software. In: 2019 International Conference on Localization and GNSS (ICL-GNSS), 4-6 June 2019, Nuremberg, Germany

https://doi.org/10.1109/ICL-GNSS.2019.8752862